Distinguishability of Quantum States by Separable Operations

Runyao Duan, Yuan Feng, Yu Xin, and Mingsheng Ying

***Abstract*— We study the distinguishability of multipartite quantum states by separable operations. We first present a necessary and sufficient condition for a finite set of orthogonal quantum states to be distinguishable by separable operations. An analytical version of this condition is derived for the case of $(D-1)$ pure states, where D is the total dimension of the state space under consideration. A number of interesting consequences of this result are then carefully investigated. Remarkably, we show there exists a large class of $2\otimes 2$ separable operations not being realizable by local operations and classical communication. Before our work only a class of $3\otimes 3$ nonlocal separable operations was known [Bennett et al, Phys. Rev. A 59, 1070 (1999)]. We also show that any basis of the orthogonal complement of a multipartite pure state is indistinguishable by separable operations if and only if this state cannot be a superposition of 1 or 2 orthogonal product states, i.e., has an orthogonal Schmidt number not less than 3, thus generalize the recent work about indistinguishable bipartite subspaces [Watrous, Phys. Rev. Lett. 95, 080505 (2005)]. Notably, we obtain an explicit construction of indistinguishable subspaces of dimension 7 (or 6) by considering a composite quantum system consisting of two qutrits (resp. three qubits), which is slightly better than the previously known indistinguishable bipartite subspace with dimension 8.**

Index Terms — **Quantum Nonlocality, Local distinguishability, Separable operations, Orthogonal Schmidt number, Unextendible Product Bases.**

I. Introduction

One of the most profound features of quantum mechanics is that composite quantum systems can exhibit nonlocality. Such an effect can be interpreted as there exist some global quantum operations performing on a composite system cannot be implemented by the owners of the subsystems using local operations and classical communication (LOCC) only. Actually, it is well known that any locally realizable quantum operation is necessarily separable. The converse part, however, is not always true, as a consequence of the weird phenomenon of "nonlocality without entanglement" discovered by Bennet and coworkers [1]. On the one hand, although many partial progresses have been made, the structure of LOCC operations is far from well understood. On the other hand, the class of separable operations is rather restricted and is with rich mathematical structure. It is relatively easier to determine whether a given quantum operation is separable by employing the well developed tools for the separability of quantum states. Thus, a deep understanding of separable operations is of particular importance in quantum information theory.

A general strategy for studying quantum nonlocality is to consider what kind of information processing tasks can be achieved by LOCC. Roughly speaking, if a certain task is accomplished with different optimal global and local efficiencies, then we can construct a class of quantum operations that cannot be realized by LOCC. Among these tasks, discrimination of orthogonal quantum states is a very effective one and has been received considerable attentions in recent years. Many interesting results have been reported, see Refs. [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28] and references therein for a partial list. There exist sets of orthogonal product states that cannot be discriminated perfectly by LOCC [1], [2], [3]; a perfect discrimination between two multipartite orthogonal quantum states can always be achieved locally [4], and this result can be generalized to the case when distinguishing two nonorthogonal states or two infinite dimensional orthogonal states [5], [6], [7], [8], [9], [10]; a complete characterization for the local distinguishability of $2\otimes 2$ states also has been obtained [11]. Despite of these significant advances, determining the local distinguishability of a finite set of orthogonal states on a multipartite state space still is a formidable task. Actually, even for an arbitrary set of multipartite orthogonal product states we still don't know how to decide the local distinguishability analytically except for the special cases of $2\otimes n$ and $3\otimes 3$, which were solved in Ref. [2] and Ref. [28], respectively.

Very recently separable operations have been widely used in order to obtain useful criteria for local distinguishability. In particular, Chefles employed separable operations as a tool to obtain a necessary and sufficient condition for a set of general quantum states to be probabilistically distinguishable by LOCC [15], see also Ref. [16]. Nathanson showed that the number of $d\otimes d$ maximally entangled states distinguishable by separable operations is at most d [17] and the same result was independently obtained by Owari and Hayashi using a slightly different method [18], which extensively generalized the results obtained by Ghosh *et al.* [19] and by Fan [20]. Watrous found a bipartite subspace with interesting property that no bases distinguishable by separable operations, and employed it to explicitly construct a class of quantum channels

This work was partly supported by the Natural Science Foundation of China (Grant Nos. 60621062 and 60503001) and the Hi-Tech Research and Development Program of China (863 project) (Grant No. 2006AA01Z102).

The material in this paper was presented in part as a long talk at the 2007 Asia Conference of Quantum Information Science (AQIS07), Kyoto, Japan. The authors are with the State Key Laboratory of Intelligent Technology and Systems, Tsinghua National Laboratory for Information Science and Technology, Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China. Yu Xin is also with the Department of Physics, Tsinghua University, Beijing 100084, China. E-mails: dry@tsinghua.edu.cn (Runyao Duan), feng-y@tsinghua.edu.cn (Yuan Feng), xiny05@mails.tsinghua.edu.cn (Yu Xin), and yingmsh@tsinghua.edu.cn (Mingsheng Ying)

with suboptimal environment-assisted capacity [21], which settled an open problem suggested by Hayden and King [22]. Hayashi *et al.* obtained a connection between the number of distinguishable states by separable operations and the average entanglement degree of the quantum states to be discriminated [23]. In Ref. [24] we studied the local distinguishability of an arbitrary basis of a multipartite state space and provided a universal tight lower bound on the number of locally unambiguously distinguishable members in an arbitrary basis. All these results suggest the following question:"What kind of quantum states can be perfectly distinguishable by separable operations?" The answer to this question will not only lead to a better understanding of the nature of separable operations, but also accelerate the present research of quantum nonlocality.

The purpose of this paper is to study the strength and the limitation of separable operations by considering the distinguishability of quantum states under separable operations. We present a necessary and sufficient condition for the distinguishability of a set of general multipartite quantum states. Assisting with this condition, we completely solve the problem of distinguishing $(D-1)$ multipartite pure states by separable operations, where D is the dimension of the multipartite state space under consideration. Two consequences are of particular interests. First we show that there exists a large class of separable operations performing on a $2\otimes 2$ quantum system cannot be realized by LOCC. This is somewhat surprising as it indicates that the capability of separable operations is much more powerful than that of LOCC operations even when only the simplest composite quantum system is under consideration, which settles an open problem recently posed by Gheorghiu and Griffiths [29] and highlights the nonlocal nature of separable operations. It is also worth noting that before our work only nonlocal separable operations acting on $3\otimes 3$ systems are known [1].

Second we show that any basis of the orthogonal complement of a multipartite pure state is indistinguishable by separable operations if and only if this state cannot be a superposition of 1 or 2 orthogonal product states, i.e., has an orthogonal Schmidt number not less than 3, thus provide a generalization of the result by Watrous [21], who proved that any basis of the orthogonal complement of a $d\otimes d$ maximally entangled state is indistinguishable by separable operations when $d\geq 3$. Furthermore, we also present an explicit construction of indistinguishable bipartite (or tripartite) subspaces of dimension 7 (resp. 6), which reduces the minimal dimension of indistinguishable bipartite subspace from 8 (given by Watrous in Ref. [21]) to 7.

Throughout this paper we consider a multipartite quantum system consisting of K parts, say $A_1,\cdots,A_K$. We assume part A_k has a state space $\mathcal{H}_k$ with dimension d_k. The whole state space is given by $\mathcal{H}=\otimes_{k=1}^K\mathcal{H}_k$ with total dimension $D=d_1\cdots d_K$. Sometimes we use the notation $d_1\otimes\cdots\otimes d_K$ for $\mathcal{H}$. With these assumptions, the rest of the paper is organized as follows. In Section II we give some necessary preliminaries, including a brief review of the notion of separable operations, the concept of generalized Schmidt number of a quantum state, and some technical lemmas. In Section III we present a necessary and sufficient condition for the distinguishability of a set of orthogonal quantum states on $\mathcal{H}$ by separable operations (Theorem 1). Many immediate but interesting consequences of this condition are discussed in details. Sections IV and V devote to the following specific problem: Let $|\Phi\rangle$ be a pure state on $\mathcal{H}$ and let $\mathcal{B}=\{|\Psi_1\rangle,\cdots,|\Psi_{D-1}\rangle\}$ be an orthonormal basis of $\{|\Phi\rangle\}^\perp$(i.e., the orthogonal complement of $|\Phi\rangle$), determine the distinguishability of $\mathcal{B}$ by separable operations. We show this problem can be solved analytically. Two special cases are most notable. The first case is concerned with two qubits, i.e., $K=2$ and $d_1=d_2=2$. We find a necessary condition for the distinguishability of $\{|\Psi_1\rangle,|\Psi_2\rangle,|\Psi_3\rangle\}$ by separable operations is that the summation of the concurrences of $|\Psi_k\rangle$ is equal to that of $|\Phi\rangle$ (Theorem 2). When $|\Phi\rangle$ is maximally entangled, such a condition is also sufficient (Corollary 2). The second case of interest is that any basis $\mathcal{B}$ of $\{|\Phi\rangle\}^\perp$ is indistinguishable by separable operations if and only if the orthogonal Schmidt number of $|\Phi\rangle$ (the least number of orthogonal product states that can linearly express $|\Phi\rangle$) is not less than 3 (Theorem 6). Section VI is of independent interest. We give an explicit construction of an indistinguishable subspace of dimension 7 (or 6) when considering a composite quantum system consisting of two qutrits (resp. three qubits). We conclude the paper in Section VII, and put some additional proofs in Appendix.

II. Preliminaries

A general quantum state ρ is characterized by its density operator, which is a positive semi-definite operator with trace one on $\mathcal{H}$. The density operator of a pure state $|\psi\rangle$ is simply the projector $|\psi\rangle\langle\psi|$. The support of ρ, denoted by $supp(\rho)$, is the vector space spanned by the eigenvectors of ρ with positive eigenvalues. Alternatively, suppose ρ can be decomposed into a convex combination of $|\psi_k\rangle\langle\psi_k|$, say,

$$\rho=\sum_{k=1}^n p_k|\psi_k\rangle\langle\psi_k|, \tag{1}$$

where $0<p_k\leq 1$ and $\sum_{k=1}^n p_k=1$. Then $supp(\rho)=span\{|\psi_k\rangle:1\leq k\leq n\}$. This fact will be extensively used without being explicitly stated. In particular, ρ is said to be separable if $|\psi_k\rangle$ can be chosen as product states.

A nonzero positive semi-definite operator E on $\mathcal{H}$ is said to be separable if the normalized form $E/\mathrm{tr}(E)$ is a separable quantum mixed state. A separable positive operator-valued measure (POVM) is a collection of semi-definite positive operators $\Pi=\{\Pi_1,\cdots,\Pi_n\}$ such that $\sum_{k=1}^n\Pi_k=I_{\mathcal{H}}$ and Π_k is separable for each $1\leq k\leq n$, where $I_{\mathcal{H}}$ is the identity operator on $\mathcal{H}$. Now we are ready to introduce the notion of separable operation. Intuitively, a separable operation is a trace-preserving completely positive linear map which sends separable states to separable ones. For completeness, we state a formal definition as follows.

Definition 1: A separable operation is a quantum operation with product Kraus operators. More precisely, a separable operation $\mathcal{E}$ acting on a multipartite state space $\mathcal{H}=\otimes_{j=1}^K\mathcal{H}_j$

should be of the following form:

$$\mathcal{E}(\rho) = \sum_{k=1}^{N} E_k \rho E_k^\dagger, \tag{2}$$

where $E_k = \otimes_{j=1}^{K} E_{kj}$ satisfies $\sum_{k=1}^{N} E_k^\dagger E_k = I$, and E_{kj} is linear operator on $\mathcal{H}_j$.

The set of separable operations is a rather restricted class of quantum operations. It is not difficult to show that any LOCC operation is separable, see Ref. [1] for a detailed discussion. However, the converse part is not true as there exists some separable operation acting on $3 \otimes 3$ cannot be implemented locally [1].

Let $\mathcal{S} = \{\rho_1, \cdots, \rho_n\}$ be a collection of n quantum states. We say that $\mathcal{S}$ is perfectly distinguishable by separable measurements if there is a separable POVM Π such that $\mathrm{tr}(\Pi_k \rho_j) = \delta_{k,j}$ for any $1 \leq k, j \leq n$. Interestingly, if a set of quantum states $\{\rho_1, \cdots, \rho_n\}$ can be perfectly distinguishable by a separable POVM Π, then we can transform this set of quantum states into another set of LOCC distinguishable states by applying a suitable separable operation $\mathcal{E}$ on the quantum system. More precisely, let $\{\sigma_1, \cdots, \sigma_n\}$ be any set of separable quantum states that can be perfectly distinguishable by LOCC, then the mentioned separable operation can be constructed as follows:

$$\mathcal{E}(\rho) = \sum_{k=1}^{n} \mathrm{tr}(\Pi_k \rho)\sigma_k. \tag{3}$$

One can easily verify that $\mathcal{E}(\rho_k) = \sigma_k$. The function of $\mathcal{E}$ can be intuitively understood as performing a separable POVM $\{\Pi_k\}$ on ρ and then preparing a separable state σ_k according to the outcome k, finally forgetting the classical information. Clearly, $\mathcal{E}$ is a separable quantum operation and can be used to perfectly discriminate the given states. Due to the above reason, when a set of states are perfectly distinguishable by a separable POVM, we directly say they are perfectly distinguishable by separable operations.

The rest of this section is to present some useful notations and technical lemmas.

Lemma 1: Let E be a positive semi-definite operator such that $0 \leq E \leq I_{\mathcal{H}}$, and let ρ be a density matrix on $\mathcal{H}$. Then $\mathrm{tr}(E\rho) = 1$ if and only if $E - P \geq 0$, where P is the projector on the support of ρ.

Proof. We first show that if $E - P \geq 0$ and $0 \leq E \leq I$, then $\mathrm{tr}(E\rho) = 1$. To see this, let $|\psi\rangle$ be any normalized vector in $supp(\rho)$. Then $\langle\psi|P|\psi\rangle = 1$. It follows from $E - P \geq 0$ that $\langle\psi|E|\psi\rangle \geq 1$. On the other hand, $E \leq I$ implies $\langle\psi|E|\psi\rangle \leq 1$. So for any $|\psi\rangle \in supp(\rho)$ we have

$$\mathrm{tr}(E|\psi\rangle\langle\psi|) = \langle\psi|E|\psi\rangle = 1.$$

Noticing that ρ can be decomposed into $\sum_{k=1}^{n} p_k |\psi_k\rangle\langle\psi_k|$ such that $|\psi_k\rangle \in supp(\rho)$ and $\sum_{k=1}^{n} p_k = 1$, we have

$$\mathrm{tr}(E\rho) = \sum_{k=1}^{n} p_k \mathrm{tr}(E|\psi_k\rangle\langle\psi_k|) = 1.$$

Conversely, $\mathrm{tr}(E\rho) = 1$ and $\langle\psi|E|\psi\rangle \leq 1$ imply that $\mathrm{tr}(E|\psi\rangle\langle\psi|) = 1$ for any normalized vector $|\psi\rangle \in supp(\rho)$. So $E|\psi\rangle = |\psi\rangle$ or $E|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|$. Noticing that $P = \sum_{k=1}^{n} |\psi_k\rangle\langle\psi_k|$ such that $\{|\psi_k\rangle\}$ is an orthonormal basis for $supp(\rho)$, then $EP = P$ and $PE = P$. Let $Q = I - P$. Then

$$E = (P + Q)E(P + Q) = P + QEQ,$$

which implies $E - P = QEQ \geq 0$. ■

We also need the following concept of Schmidt number of a quantum state.

Definition 2: The *Schmidt number* of a multipartite quantum state ρ, denoted by $Sch(\rho)$, is the minimal number of product pure states whose linear span contains $supp(\rho)$. The *orthogonal Schmidt number* of ρ, denoted by $Sch_\perp(\rho)$, can be defined similarly with the additional requirement that these product pure states should be mutually orthogonal.

For pure state $|\Psi\rangle$ the (orthogonal) Schmidt number is exactly reduced to the minimal number of (orthogonal) pure product states needed to express $|\Psi\rangle$ as a superposition and this is just the definition given by Eisert and Briegel [30]. It is difficult to determine the Schmidt number of a general multipartite state. Only for bipartite pure states and some special multi-qubit states the Schmidt number can be analytically determined [30], [31]. We should point out that the definition of Schmidt number given here does not coincide with the one given by Terhal and Horodecki [32].

By definition, we have the following useful fact:

$$Sch(\rho) \geq \max\{Sch(\Psi) : |\Psi\rangle \in supp(\rho)\}. \tag{4}$$

This inequality can be used to provide a lower bound for $Sch(\rho)$.

It is interesting that the Schmidt number provides a simple criterion for the separability. In fact, when ρ is separable, $supp(\rho)$ can be spanned by a set of product states. Thus we have:

Lemma 2: For any quantum state ρ, $R(\rho) \leq Sch(\rho)$, where $R(\rho)$ is the rank of ρ. The equality holds if ρ is separable.

A typical use of Lemma 2 is to show a quantum state ρ is entangled. Usually this can be achieved by finding a vector $|\Psi\rangle$ in $supp(\rho)$ such that $Sch(\Psi) > R(\rho)$.

The Schmidt decomposition of a bipartite pure state is not unique. However, when multipartite pure states with Schmidt number 2 are under consideration, we do have a unique decomposition. Let $|a\rangle = \otimes_{k=1}^{K} |a_k\rangle$ and $|b\rangle = \otimes_{k=1}^{K} |b_k\rangle$ be product vectors on $\mathcal{H} = \otimes_{k=1}^{K} \mathcal{H}_k$. Then $|a\rangle$ and $|b\rangle$ are said to be different at the k-th entry if $|a_k\rangle \neq z|b_k\rangle$ for any complex number z. Let $h(|a\rangle, |b\rangle)$ be the total number of different entries between $|a\rangle$ and $|b\rangle$. Then we have the following interesting result.

Lemma 3: Let $|\Phi\rangle = |a\rangle + |b\rangle$ be an entangled state of $\mathcal{H}$ such that $h(|a\rangle, |b\rangle) \geq 3$. Then there cannot exist product vectors $|c\rangle$ and $|d\rangle$ such that $|\Phi\rangle = |c\rangle + |d\rangle$ and $\{|a\rangle, |b\rangle\} \neq \{|c\rangle, |d\rangle\}$. In other words, $|\Phi\rangle$ has a unique Schmidt decomposition.

Proof. Without loss of generality, assume $h(|a\rangle, |b\rangle) = 3$. By contradiction, suppose there exist another two product vectors $|c\rangle$ and $|d\rangle$ which also yield a decomposition of $|\Phi\rangle$. That is,

$$|a_1 a_2 a_3\rangle + |b_1 b_2 b_3\rangle = |c_1 c_2 c_3\rangle + |d_1 d_2 d_3\rangle, \tag{5}$$

where a_k is not equal to b_k for each $1 \leq k \leq 3$. Let $|a_1^\perp\rangle \in span\{|a_1\rangle, |b_1\rangle\}$ such that $\langle a_1^\perp|a_1\rangle = 0$ and $\langle a_1^\perp|b_1\rangle \neq 0$. Then multiplying $\langle a_1^\perp|$ on the both sides of the above equation we have that $|b_2b_3\rangle$ is contained in $S = span\{|c_2c_3\rangle, |d_2d_3\rangle\}$. Similarly we can also show $|a_2a_2\rangle \in S$. On the other hand, there are only two unique product vectors $|c_2c_3\rangle$ and $|d_2d_3\rangle$ in S (up to some factors). Then it follows that $\{|a_2a_3\rangle, |b_2b_3\rangle\}$ is essentially $\{|c_2c_3\rangle, |d_2d_3\rangle\}$. Without loss of generality, assume $|a_2a_3\rangle = \alpha|c_2c_3\rangle$ and $|b_2b_3\rangle = \beta|d_2d_3\rangle$ for some complex numbers α and β, then

$$(\alpha|a_1\rangle - |c_1\rangle)|c_2c_3\rangle + (\beta|b_1\rangle - |d_1\rangle)|d_2d_3\rangle = 0, \quad (6)$$

which is possible if and only if $|a_1\rangle = \alpha^{-1}|c_1\rangle$ and $|b_1\rangle = \beta^{-1}|d_1\rangle$. That also means $|a\rangle = |c\rangle$ and $|b\rangle = |d\rangle$. A contradiction with our assumption. ■

We also need the following result concerning with the separability of rank 2 positive semi-definite operators.

Lemma 4: Let $|\Psi\rangle$ and $|\Phi\rangle$ be pure states on $\mathcal{H}$ and $\lambda \geq 0$. Then $\rho(\lambda) = |\Psi\rangle\langle\Psi| + \lambda|\Phi\rangle\langle\Phi|$ is separable if and only if one of the following cases holds:

(i) Both $|\Psi\rangle$ and $|\Phi\rangle$ are product states and $\lambda \geq 0$;

(ii) $|\Psi\rangle$ is a product state and $\lambda = 0$;

(iii) There are two product states $|a\rangle$ and $|b\rangle$ and positive real numbers α, β, γ, δ such that $|\Psi\rangle = \alpha|a\rangle + \beta|b\rangle$, $|\Phi\rangle = \gamma|a\rangle - \delta|b\rangle$, and $\lambda = \alpha\beta/\gamma\delta$. (There may be some global phase factors before $|\Psi\rangle$ and $|\Phi\rangle$.)

Proof. By a direct calculation one can readily verify that (i), (ii) and (iii) are sufficient for the separability of $\rho(\lambda)$. We only need to show that they are also necessary. The case that both states are unentangled is trivial, corresponding to (i). We shall consider the following two cases only:

(1) One of $|\Psi\rangle$ and $|\Phi\rangle$ is entangled. First assume that $|\Phi\rangle$ is entangled. Then for any $\lambda > 0$. $\rho(\lambda)$ is just a mixture of an entangled state and a product state, and should be entangled for any $\lambda > 0$, as shown by Horodecki *et al.* [34]. So the only possible case is $\lambda = 0$, i.e., (ii) holds. Second, when $|\Psi\rangle$ is entangled we can show by a similar argument that $\rho(\lambda)$ cannot be separable for any $\lambda \geq 0$.

(2) Both states are entangled. We shall show that condition (iii) is necessary. Suppose that $\rho(\lambda)$ is separable, then by Lemma 2, it follows that $Sch(\rho(\lambda)) = R(\rho(\lambda)) = 2$. In other words, the support of $\rho(\lambda)$ can be spanned by two product states $|a\rangle$ and $|b\rangle$. Noticing that both $|\Psi\rangle$ and $|\Phi\rangle$ are contained in the support of $\rho(\lambda)$, we can write

$$|\Psi\rangle = \alpha|a\rangle + \beta|b\rangle, \quad (7)$$

$$|\Phi\rangle = \gamma|a\rangle + \delta|b\rangle \quad (8)$$

for nonzero complex numbers $\alpha, \beta, \gamma, \delta$. Furthermore, $|a\rangle$ and $|b\rangle$ are also the only product states in $supp(\rho(\lambda))$. So $\rho(\lambda)$ should be a mixture of $|a\rangle\langle a|$ and $|b\rangle\langle b|$. Substituting $|\Psi\rangle$ and $|\Phi\rangle$ into $\rho(\lambda)$ and setting the coefficients of $|a\rangle\langle b|$ and $|b\rangle\langle a|$ to be zero we have

$$\alpha\beta^* + \lambda\gamma\delta^* = 0. \quad (9)$$

By adding suitable phase factors before $|\Psi\rangle$ and $|\Phi\rangle$, we can make α and γ positive. The condition $\lambda > 0$ implies that $\beta = |\beta|e^{i\theta}$ and $\delta = -|\delta|e^{i\theta}$ for some real number θ. Absorbing the phase factor $e^{i\theta}$ into $|b\rangle$ and resetting β and δ to $|\beta|$ and $-|\delta|$ respectively, we know that condition (iii) is satisfied. ■

III. Conditions for the distinguishability of quantum states by separable operations

It would be desirable to know when a collection of quantum states is perfectly distinguishable by separable operations. Orthogonality is generally not sufficient for the existence of a separable POVM for discrimination. A rather simple but useful necessary and sufficient condition is as follows.

Theorem 1: Let $\mathcal{S} = \{\rho_1, \cdots, \rho_n\}$ be a collection of orthogonal quantum states of $\mathcal{H}$. Then $\mathcal{S}$ is perfectly distinguishable by separable operations if and only if there exist n positive semi-definite operators $\{E_1, \cdots, E_n\}$ such that $P_k + E_k$ is separable for each $1 \leq k \leq n$, and $\sum_{k=1}^n E_k = P_0$, where P_k is the projector on $supp(\rho_k)$, and $P_0 = I_{\mathcal{H}} - \sum_{k=1}^n P_k$.

Proof. Sufficiency is obvious. Suppose that (ii) holds, let us define a POVM $\Pi = \{\Pi_1, \cdots, \Pi_n\}$ as follows: $\Pi_k = P_k + E_k$ for each $1 \leq k \leq n$. It is easy to verify that Π is a separable measurement that perfectly discriminates $\mathcal{S}$.

Now we turn to show the necessity. Suppose $\mathcal{S}$ is perfectly distinguishable by some separable POVM, say $\{\Pi_1, \cdots, \Pi_n\}$. Take $E_k = \Pi_k - P_k$ for each $1 \leq k \leq n$. Then $\sum_{k=1}^n E_k = P_0$. To complete the proof, it suffices to show $E_k \geq 0$. By the assumption, we have $\mathrm{tr}(\Pi_k\rho_k) = 1$. Then the positivity of E_k follows directly from Lemma 1. ■

In some sense Theorem 1 is only a reformulation of our discrimination problem. One may doubt it can provide any valuable results. However, this seemingly trivial reformulation does give us much more operational forms of the measurement operators for discrimination and connects them to the separability problem, which is one of the central topics in quantum information theory and has been extensively studied since the last two decades. So many well developed tools for the separability problem may be applicable in the context of discrimination. As a result, Theorem 1 is unexpectedly powerful.

Some special but interesting cases of Theorem 1 deserve careful investigations. When the supports of the states in $\mathcal{S}$ together span the whole state space, i.e., $supp(\sum_{k=1}^n \rho_k) = \mathcal{H}$, $\mathcal{S}$ is perfectly distinguishable by separable operations if and only if P_k is separable for each $1 \leq k \leq n$. In particular, an orthonormal basis of $\mathcal{H}$ is perfectly distinguishable by separable operations if and only if it is a product basis, which is a well known result first obtained by Horodecki *et al.* using a rather different method [25], see also [15] for another simple proof.

A slightly more general case is when there exists k such $P_0 + P_k$ and P_j are all separable for any $j \neq k$. In this case we say that $\{P_j : j \neq k\}$ is completable [33]. It has been shown in Ref. [2] that a sufficient condition for a set of orthogonal product states to be completable is that they are exactly distinguishable by LOCC. Combining this with Theorem 1, we have the following interesting corollary:

Corollary 1: A set of LOCC distinguishable product states together with any state in its orthogonal complement is always perfectly distinguishable by separable operations.

We notice that DiVincenzo and co-workers have shown in Ref. [3] that any three (or four) orthogonal multipartite (resp. bipartite) product states are distinguishable by LOCC. Hence we conclude immediately by the above corollary that any four (or five) orthogonal multipartite (resp. bipartite) states including three (resp. four) product states are perfectly distinguishable by separable operations. The case when $\mathcal{S}$ is a set of product states is of particular interest and has been studied carefully in Ref. [3] using a rather different method. Specifically, let $\mathcal{S} = \{|\psi_1\rangle, \cdots, |\psi_n\rangle\}$. Then it has been shown that if $S_k = S - \{|\psi_k\rangle\}$ is completable for each $1 \leq k \leq n$, then S is perfectly distinguishable by separable operations. Interesting examples include any orthogonal UPB consisting of four $2 \otimes 2 \otimes 2$ (or five $3 \otimes 3$) product states. Clearly we have refined the results by DiVincenzo *et al.*

As another important consequence of Theorem 1, we shall show that the problem of distinguishing $(D-1)$ orthogonal pure states by separable operations can be completely solved. Notice that if $|\Phi\rangle$ is a product state, then the only form of $\mathcal{B}$ that can be distinguishable by separable operations is a product basis. For simplicity, in what follows we shall assume $|\Phi\rangle$ is an entangled state. We shall consider two cases $Sch_\perp(\Phi) = 2$ and $Sch_\perp(\Phi) \geq 3$ respectively in the next two sections.

IV. Distinguishability of arbitrary orthonormal basis of $\{|\Phi\rangle\}^\perp$ with $Sch_\perp(\Phi) = 2$

We start with the simplest $2 \otimes 2$ case and provide an analytical solution. It is well known that any $2 \otimes 2$ state $|\Psi\rangle$ can be uniquely represented by a 2×2 matrix Ψ as follows:

$$|\Psi\rangle = (I \otimes \Psi)|\Phi_+\rangle, \tag{10}$$

where $|\Phi_+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$ is a maximally entangled state. The *concurrence* of $|\Psi\rangle$ is given by the absolute value of the determinant of Ψ, i.e., $C(\Psi) = |\det(\Psi)|$. This rewriting form coincides with the original definition given by Wootters [35]. So $0 \leq C(\Psi) \leq 1$ for any $2 \otimes 2$ state $|\Psi\rangle$. In particular, $C(\Psi)$ vanishes for product states while attains one for maximally entangled states. We say complex numbers z_1 and z_2 are anti-parallel if there exists a negative real number a such that $z_1 = az_2$. First we need the following simplified version of Lemma 4 in the $2 \otimes 2$ case.

Lemma 5: Let $|\Psi\rangle$ and $|\Phi\rangle$ be two $2 \otimes 2$ entangled pure states, and let $\lambda \geq 0$. Then $\rho(\lambda) = |\Psi\rangle\langle\Psi| + \lambda|\Phi\rangle\langle\Phi|$ is separable if and only if $\Psi\Phi^{-1}$ has two anti-parallel eigenvalues and $\lambda = C(\Psi)/C(\Phi)$. Note that $|\Phi\rangle$ is entangled implies that Φ is invertible.

Now the distinguishability of three $2 \otimes 2$ orthogonal states by separable operations is characterized as follows.

Theorem 2: Let $|\Phi\rangle$ be a $2 \otimes 2$ pure state, and let $\mathcal{B} = \{|\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ be an orthonormal basis for $\{|\Phi\rangle\}^\perp$. Then $\mathcal{B}$ is perfectly distinguishable by separable operations if and only if (i) $\Psi_k\Phi^{-1}$ has two anti-parallel eigenvalues for each entangled state Ψ_k; and (ii) $C(\Psi_1)+C(\Psi_2)+C(\Psi_3) = C(\Phi)$.

Proof. By Theorem 1, the POVM element that can perfectly identify $|\Psi_k\rangle$ should have the form $\Pi_k = |\Psi_k\rangle\langle\Psi_k| + \lambda_k|\Phi\rangle\langle\Phi|$, where $0 \leq \lambda_k \leq 1$ and $\lambda_1 + \lambda_2 + \lambda_3 = 1$. If $|\Psi_k\rangle$ is a product state, then it follows from Lemma 4 that Π_k is separable if and only if $\lambda_k = 0$. Otherwise by Lemma 5 we have that Π_k is separable if and only if $\Psi_k\Phi^{-1}$ has two anti-parallel eigenvalues and $\lambda_k = C(\Psi_k)/C(\Phi)$. So by $\lambda_1+\lambda_2+\lambda_3 = 1$ we have $C(\Psi_1)+C(\Psi_2)+C(\Psi_3) = C(\Phi)$. That completes the proof. ■

The most interesting part in the above theorem is Condition (ii). It reveals a precise relation between the concurrences and the distinguishability by separable operations. By a careful observation, we notice that a similar condition has been previously obtained by Hayashi et al. in Ref. [23], where a very general relation between distinguishability by separable operations and average entanglement degree of the states to be discriminated was presented. When only $2 \otimes 2$ states were involved, this relation can be reduced to an inequality similar to condition (ii). The key difference is that here what we obtained is an exact identity that (almost) completely characterizes the distinguishability by separable operations.

Suppose now $|\Phi\rangle$ is maximally entangled. Then $\Phi = U$ for some 2×2 unitary matrix. Noticing that

$$\mathrm{tr}(\Psi_k\Phi^{-1}) = \mathrm{tr}(U^\dagger\Psi_k) = 2\langle\Phi|\Psi_k\rangle = 0$$

for $k = 1, 2, 3$, we conclude that $\Psi_k\Phi^{-1}$ should have two anti-parallel eigenvalues (assume that $|\Psi_k\rangle$ is entangled). Furthermore, the concurrence of a $2 \otimes 2$ maximally entangled state is one. Collecting all these facts together we have the following interesting corollary:

Corollary 2: Let $|\Phi\rangle$ be a $2 \otimes 2$ maximally entangled state, and let $\mathcal{B} = \{|\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ be an orthonormal basis for $\{|\Phi\rangle\}^\perp$. Then $\mathcal{B}$ is perfectly distinguishable by separable operations if and only if $C(\Psi_1) + C(\Psi_2) + C(\Psi_3) = 1$.

Theorem 2 implies that there exists a large class of $2 \otimes 2$ separable operations that cannot be implemented locally. We shall exhibit an explicit construction of such separable operations. We achieve this goal by identifying a set of states that is distinguishable by separable operations but is not LOCC distinguishable.

Let $|\Psi(\theta)\rangle = \cos\theta|01\rangle + \sin\theta|10\rangle$ and $|\Phi(\theta)\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ for $\theta \in \mathcal{R}$. Then for any $0 < \alpha \leq \beta \leq \pi/4$, let $|\Phi\rangle = |\Phi(\beta)\rangle$, and let $|\Psi_1\rangle = |\Psi(\alpha)\rangle$, $|\Psi_2\rangle = \cos\gamma|\Psi(\alpha - \frac{\pi}{2})\rangle + \sin\gamma|\Phi(\beta - \frac{\pi}{2})\rangle$, $|\Psi_3\rangle = \sin\gamma|\Psi(\alpha - \frac{\pi}{2})\rangle - \cos\gamma|\Phi(\beta - \frac{\pi}{2})\rangle$ be an orthonormal basis of $\{|\Phi\rangle\}^\perp$. Choose γ such that

$$\tan^{-1}\sqrt{\frac{\sin 2\alpha}{\sin 2\beta}} \leq \gamma \leq \tan^{-1}\sqrt{\frac{\sin 2\beta}{\sin 2\alpha}}. \tag{11}$$

By direct calculations we can easily verify that the assumptions of Theorem 2 are fulfilled, thus $\mathcal{B} = \{|\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ is perfectly distinguishable using separable operations. However, it is clear whenever $0 < \alpha < \beta \leq \frac{\pi}{4}$, both $|\Psi_1\rangle$ and $|\Psi_2\rangle$ are entangled, thus $\mathcal{B}$ is indistinguishable by LOCC, as shown by Walgate and Hardy [11]. Interestingly, $|\Psi_3\rangle$ is reduced to a product state when γ takes one of the extreme values in Eq. (11).

The above example also implies that the distinguishability by separable operations has some continuous property. We formalize this intuitive observation as follows:

Theorem 3: Let c_1, c_2, c_3 be nonnegative real numbers such that $0 \leq c_1+c_2+c_3 \leq 1$. Then there exists a set of three $2 \otimes 2$

states $\{|\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ satisfying (i) $C(\Psi_k) = c_k$ for $k = 1, 2, 3$; and (ii) $\{|\Psi_1\rangle, |\Psi_2\rangle, |\Psi_3\rangle\}$ is perfectly distinguishable by separable operations.

There is a nice geometrical way to illustrate the distinguishability of quantum states by different class of operations. To see this, we identify a triple of orthogonal quantum states $(|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle)$ by a point $(C(\psi_1), C(\psi_2), C(\psi_3))$ of R^3. We say such a point is distinguishable by global (or separable, LOCC) operations if the related states are distinguishable by the corresponding operations. By a careful analysis, we can show any point in the regular tetrahedron in Fig. 1 corresponds to some orthonormal basis of $\{|\Phi_+\rangle\}^\perp$. A detailed proof for this interesting fact is given in the Appendix A. So the points in the regular tetrahedron represent a region that can be perfectly distinguishable by global quantum operations. The yellow triangle BCD is exactly the set of points distinguishable by separable operations. Finally, three vertices B, C, and D are the only points that are distinguishable by LOCC. From such a representation we can clearly see that the class of $2 \otimes 2$ separable operations strictly lies between the classes of LOCC and global operations.

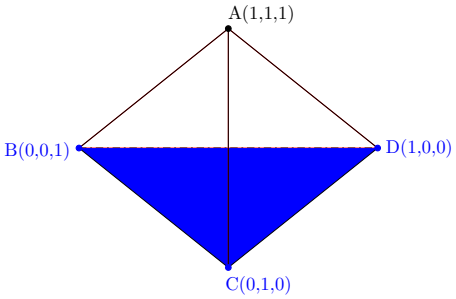

Fig. 1. Illustration of the distinguishability of the basis of $\{|\Phi_+\rangle\}^\perp$, where $|\Phi_+\rangle$ is a $2 \otimes 2$ maximally entangled states and we identify an orthonormal basis $(|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle)$ by a point $(C(\psi_1), C(\psi_2), C(\psi_3))$ in R^3. Any point in the regular tetrahedron ABCD corresponds a legal orthonormal basis of $\{|\Phi_+\rangle\}^\perp$, thus is distinguishable by global operations. Vertices B, C, and D are the only points corresponding to LOCC distinguishable basis. Interestingly, the triangle $\triangle BCD$ represents bases that are distinguishable by separable operations.

Now we consider the multipartite setting. There are two possible cases: $|\Phi\rangle$ is reduced to a bipartite entangled state only between two parties; or $|\Phi\rangle$ is an entangled state at least between three parties. The following two theorems deal with these two cases separately. Surprisingly, the first case is essentially reduced to $2 \otimes 2$ case.

Theorem 4: Let $|\Phi\rangle = |a_1 \cdots a_{K-2}\rangle|\Phi'\rangle$ be a pure state on $\mathcal{H}$ such that $|\Phi'\rangle$ is an entangled state between parties A_{K-1} and A_K. Then $\mathcal{B}$ is perfectly distinguishable by separable operations if and only if each entangled state $|\Psi\rangle$ in $\mathcal{B}$ can be written into the form $|\Psi\rangle = |a_1 \cdots a_{K-2}\rangle|\Psi'\rangle$ for some bipartite entangled state $|\Psi'\rangle$ between A_{K-1} and A_K such that (i) all $|\Psi'\rangle$ and $|\Phi'\rangle$ can be embeded into a $2 \otimes 2$ subspace $\mathcal{H}'$ of $\mathcal{H}_{K-1} \otimes \mathcal{H}_K$; and (ii) $\Psi'\Phi'^{-1}$ has two anti-parallel eigenvalues and $\sum_{\Psi'} C(\Psi') = C(\Phi')$, where Ψ' and Φ' are $2 \otimes 2$ matrices that are the representations of $|\Psi'\rangle$ and $|\Phi'\rangle$ on $\mathcal{H}'$ in the sense of Eq. (10), respectively.

Proof. Let $|\Psi\rangle$ be any entangled state of $\mathcal{B}$. Then there is some $0 < \lambda \leq 1$ such that $|\Psi\rangle\langle\Psi| + \lambda|\Phi\rangle\langle\Phi|$ is separable. According to the assumptions on $|\Phi\rangle$ and employing Lemma 4, we can easily see that $|\Psi\rangle$ should be of the form $|b_1 \cdots b_{K-2}\rangle \otimes |\Psi'\rangle$. Second, we have $|a_1 \cdots a_{K-2}\rangle$ should be identical to $|b_1 \cdots b_{K-2}\rangle$ up to some factors. Otherwise $span\{|\Psi\rangle, |\Phi\rangle\}$ cannot contain product states. So we need $|\Psi'\rangle\langle\Psi'| + \lambda|\Phi'\rangle\langle\Phi'|$ being separable. Now the problem is reduced to the $2 \otimes 2$ case and the result follows directly from Theorem 2. ■

The case that $|\Phi\rangle$ is at least entangled among three parties is much more simple. Any distinguishable basis should contain a unique entangled state with a predetermined form.

Theorem 5: Let $|\Phi\rangle = \cos\theta|a\rangle + \sin\theta|b\rangle$ be an entangled pure state of $\mathcal{H}$ such that $\langle a|b\rangle = 0$ and $h(|a\rangle, |b\rangle) \geq 3$. Then $\mathcal{B}$ can be perfectly distinguishable by separable operations if and only if there is a unique entangled state $|\Psi\rangle$ in $\mathcal{B}$ with the form $|\Psi\rangle = \sin\theta|a\rangle - \cos\theta|b\rangle$, and the other states should form an orthogonal product basis of $\{|a\rangle, |b\rangle\}^\perp$.

Proof. Sufficiency is obvious. We only consider the necessity. Suppose that $\mathcal{B}$ is distinguishable by separable operations. Noticing that $|\Phi\rangle$ is entangled, we conclude that $\mathcal{B}$ should contain at least one entangled state. By Lemma 3, one can easily show that any entangled state $|\Psi\rangle$ such that $|\Psi\rangle\langle\Psi| + \lambda|\Phi\rangle\langle\Phi|$ is separable should be contained in $span\{|a\rangle, |b\rangle\}$. Noticing that $|\Psi\rangle$ is orthogonal to $|\Phi\rangle$, we can deduce that $|\Psi\rangle$ is uniquely determined and is given by $\sin\theta|a\rangle - \cos\theta|b\rangle$. ■

V. $\{|\Phi\rangle\}^\perp$ HAS NO BASES DISTINGUISHABLE BY SEPARABLE OPERATIONS WHEN $Sch_\perp(\Phi) \geq 3$

Now we consider the case when $Sch_\perp(\Phi) \geq 3$. Our result is a generalization of Watrous's result. It is remarkable that the orthogonal Schmidt number of $|\Phi\rangle$ completely characterizes the distinguishability of the subspace $\{|\Phi\rangle\}^\perp$.

Theorem 6: Let $|\Phi\rangle$ be an entangled pure state on $\mathcal{H}$. Then $\{|\Phi\rangle\}^\perp$ having no orthonormal basis perfectly distinguishable by separable operations if and only if $Sch_\perp(\Phi) > 2$. In particular, when $Sch_\perp(\Phi) = 2$, there always exists an orthonormal basis $\mathcal{B}$ of $\{|\Phi\rangle\}^\perp$ that is perfectly distinguishable by LOCC.

Proof. Necessity: Suppose $Sch_\perp(\Phi) = 2$. Then the existence of a distinguishable basis by separable operations follows directly from Theorem 4. Here we further construct a basis for $\{|\Phi\rangle\}^\perp$ that is distinguishable by LOCC. Notice that $|\Phi\rangle$ can be written into the form $|\Phi\rangle = \cos\theta|\Phi_0\rangle + \sin\theta|\Phi_1\rangle$, where $|\Phi_0\rangle$ and $|\Phi_1\rangle$ are orthogonal product states on $\mathcal{H}$ and $0 < \theta < \pi/2$. Then we can extend $|\Phi_0\rangle$ and $|\Phi_1\rangle$ into a complete orthogonal product basis $\{|\Phi_0\rangle, |\Phi_1\rangle, \cdots, |\Phi_{D-1}\rangle\}$ of $\mathcal{H}$. We can further assume this basis is distinguishable by local projective measurements [2]. Replacing $|\Phi_0\rangle$ and $|\Phi_1\rangle$ with $|\Psi\rangle = \sin\theta|\Phi_0\rangle - \cos\theta|\Phi_1\rangle$ we obtain a basis for $\{|\Phi\rangle\}^\perp$ that is distinguishable by the same local projective measurements.

Sufficiency: In this case we have $Sch_\perp(\Phi) \geq 3$. If $Sch(\Phi) \geq 3$. Then for any $\lambda_k > 0$ we know from Lemma 4 that $\Pi(\lambda_k) = |\Psi_k\rangle\langle\Psi_k| + \lambda_k|\Phi\rangle\langle\Phi|$ should be entangled. That implies any basis of $\{|\Phi\rangle\}^\perp$ is indistinguishable by separable operations.

Suppose now that $Sch_\perp(\Phi) \geq 3$ and $Sch(\Phi) = 2$. By contradiction, assume there exists a basis $\mathcal{B}$ distinguishable

by separable operations. Then applying Lemma 3, we know there are two unique product vectors $|a\rangle$ and $|b\rangle$ such that $|\Phi\rangle = |a\rangle + |b\rangle$. So any state $|\Psi_k\rangle$ with $\lambda_k > 0$ should also be a superposition of $|a\rangle$ and $|b\rangle$. As there are only two orthogonal states in $span\{|a\rangle, |b\rangle\}$, we conclude the only possibility is that there is a unique state $|\Psi_k\rangle$ with $\lambda_k = 1$ and all the other states are product states. On the other hand, let $|\Psi\rangle$ be the entangled state in $span\{|a\rangle, |b\rangle\}$ such that $\langle\Psi|a\rangle = 0$. Then

$$|\Psi_k\rangle\langle\Psi_k| + |\Phi\rangle\langle\Phi| = |a\rangle\langle a| + |\Psi\rangle\langle\Psi| \tag{12}$$

is separable. But the right hand side of the above equation is a summation of an entangled state and a product state, it should be entangled [34]. A contradiction. ■

Let us check some interesting examples. Take $|\Phi\rangle$ to be a W-type state, $|\Phi\rangle = a|001\rangle + b|010\rangle + c|100\rangle$, where $|a|^2 + |b|^2 + |c|^2 = 1$, and $abc \neq 0$. Then $Sch_\perp(\Phi) = Sch(\Phi) = 3$. It follows from Theorem 6 that any orthonormal basis of $\{|\Phi\rangle\}^\perp$ cannot be perfectly distinguishable by separable operations. This yields an indistinguishable subspace with dimension $2^3 - 1 = 7$, which is a slight improvement over the bipartite case, where a $3 \otimes 3$ indistinguishable subspace of dimension 8 was given by Watrous [21]. But if we choose the GHZ-type state $|\Phi\rangle = \cos\theta|000\rangle + \sin\theta|111\rangle$, where $0 \leq \theta \leq \frac{\pi}{2}$. Then $\{|\Phi\rangle\}^\perp$ does have an orthonormal basis that is perfectly distinguishable by LOCC. Interestingly, if we take $|\Phi\rangle = \alpha|000\rangle + \beta|{+}{+}{+}\rangle$, where $\alpha\beta \neq 0$ and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Then we can easily see that $Sch(\Phi) = 2$ but $Sch_\perp(\Phi) \geq 3$, as $|\Phi\rangle$ cannot be written into a superposition of two orthogonal product states. Thus it follows from the above theorem that $\{|\Phi\rangle\}^\perp$ does not have any orthonormal basis distinguishable by separable operations.

VI. Indistinguishable subspaces with smaller dimensions

The dimension of indistinguishable subspaces can be further reduced. We shall show that there exist a $3\otimes3$ indistinguishable subspace with dimension 7 and a $2 \otimes 2 \otimes 2$ indistinguishable subspace with dimension 6. We first consider bipartite case. Let $|\Phi_1\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ and $|\Phi_2\rangle = |01\rangle$. Let $S = span\{|\Phi_1\rangle, |\Phi_2\rangle\}$. It is clear that $S^\perp$ is a bipartite subspace with dimension 7. Surprisingly, we have the following interesting result:

Theorem 7: $S^\perp$ is indistinguishable by separable operations.

Proof. We need the following easily verifiable properties of S to complete the proof:

P0: $|\Phi_2\rangle$ is the unique product vector (up to a scalar factor) in S;

P1. $Sch(\Psi) = 3$ for any entangled state $|\Psi\rangle \in S$;

P2. Any positive operator ρ such that $supp(\rho) = S$ satisfies $Sch(\rho) = 4$.

The validity of P0 can be directly verified. We only consider P1 and P2. We first show the validity of P1. Actually, any entangled state $|\psi\rangle$ from S can be written into a superposition of $|\Phi_1\rangle$ and $|\Phi_2\rangle$. That is,

$$|\psi\rangle = \alpha|\Phi_1\rangle + \beta|\Phi_2\rangle, \tag{13}$$

where $\alpha \neq 0$ and $|\alpha|^2 + |\beta|^2 = 1$. Substituting $|\Phi_1\rangle$ and $|\Phi_2\rangle$ into the above equation, we have

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|0\rangle(\alpha|0\rangle + \sqrt{3}\beta|1\rangle) + \alpha|11\rangle + \alpha|22\rangle), \tag{14}$$

which is clearly an entangled state with Schmidt number 3 for any $\alpha \neq 0$.

Now we turn to show the validity of P2. By contradiction, suppose for some ρ such that $supp(\rho) = S$ we have $Sch(\rho) = 3$. Then there should exist three unnormalized product states $|a_1b_1\rangle$,$|a_2b_2\rangle$, and $|a_3b_3\rangle$ such that

$$|\Phi_1\rangle = |a_1b_1\rangle + |a_2b_2\rangle + |a_3b_3\rangle, \tag{15}$$

$$|\Phi_2\rangle = \alpha_1|a_1b_1\rangle + \alpha_2|a_2b_2\rangle + \alpha_3|a_3b_3\rangle. \tag{16}$$

Without loss of generality, we may assume $\alpha_1 \neq 0$. Then it is clear that

$$|\Phi_1\rangle - \alpha_1^{-1}|\Phi_2\rangle = (1 - \frac{\alpha_2}{\alpha_1})|a_2b_2\rangle + (1 - \frac{\alpha_3}{\alpha_1})|a_3b_3\rangle. \tag{17}$$

By P1, the left hand side of the above equation has Schmidt number 3, while the right hand side of the above equation has Schmidt number at most 2. That is a contradiction.

Now let $\mathcal{B} = \{|\Psi_k\rangle : 1 \leq k \leq 7\}$ be any orthogonal basis of $S^\perp$. By Theorem 1, the POVM element identifying $|\Psi_k\rangle$ is of the form $\Pi_k = |\Psi_k\rangle\langle\Psi_k| + E_k$, where $\sum_{k=1}^7 E_k = |\Phi_1\rangle\langle\Phi_1| + |\Phi_2\rangle\langle\Phi_2|$ and $E_k \geq 0$.

So we can choose E_k such that $E_k \neq 0$ and $E_k \neq |01\rangle\langle 01|$ (up to some factor). We shall show that Π_k should be entangled. There are two cases. If $R(E_k) = 1$ then by P1 we have $Sch(E_k) = 3$, which follows that $Sch(\Pi_k) \geq 3 > R(\Pi_k)$. Similarly, if $R(E_k) = 2$ then by P2 we have $Sch(\Pi_k) \geq Sch(E_k) = 4 > R(\Pi_k)$. In both cases Π_k is entangled. That completes the proof. ■

Using the very same method, we can construct a $2\otimes2\otimes2$ indistinguishable subspace with dimension 6. For instance, take $|\Phi_1\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{3}$ and $|\Phi_2\rangle = |000\rangle$. Then $\{|\Phi_1\rangle, |\Phi_2\rangle\}^\perp$ is indistinguishable by separable operations.

VII. Conclusions

In summary, we provided a necessary and sufficient condition for the distinguishability of a set of multipartite quantum states by separable operations. A set of three $2 \otimes 2$ pure states that is perfectly distinguishable by separable operations but is indistinguishable by LOCC then was explicitly constructed. As a consequence, there exists a large class of nonlocal separable operations even for the simplest composite quantum system consisting of two qubits. We also showed that the orthogonal complement of a pure state has no bases distinguishable by separable operations if and only if this state has an orthogonal Schmidt number not less than 3. We believe these results would be useful in clarifying the relation between separable operations and LOCC.

There are still a number of unsolved problems that are worthwhile for further study. We have mentioned some in the previous context. Here we would like to stress two of them. The first one is concerning with the distinguishability of orthogonal product pure states. It a simple fact that any set of orthogonal product pure states can be perfectly distinguishable

by some positive-partial-transpose preserving (PPT) operation. Is this also true for separable operations? We have seen that separable operations are powerful enough to distinguish any set of orthogonal product pure states in $3\otimes3$ and $2\otimes2\otimes2$. If the answer is affirmative in general, then how to prove? Otherwise a counterexample would be highly desirable. With little effort we can easily show that it is sufficient to verify whether any UPB is perfectly distinguishable by separable operations. The difficulty we met is that the structure of UPB on a multipartite state space remains unknown except for some special cases.

Another problem is to find more applications of locally indistinguishable subspaces (LIS). The work of Watrous suggests that bipartite LIS can be used to construct quantum channels with sub-optimal environment-assisted capacity. It would be of great interest to employ LIS as a tool to give tighter upper of the capacity. In the asymptotic setting similar problem has been thoroughly studied by Winter [36]. Hopefully, these efforts would reveal some deep properties of LIS and testify the richness of the mathematical structure of this notion.

Appendix: Geometric representation of the concurrences of orthogonal bases of $\{|\Phi\rangle\}^\perp$

First we recall a useful representation of the concurrence of a two-qubit pure state. Let $\{|\Phi_k\rangle : 1 \leq k \leq 4\}$ be the magic basis [35], and let $|\psi\rangle$ be any pure state such that $|\psi\rangle = \sum_{k=1}^4 \lambda_k |\Phi_k\rangle$. Then the concurrence of $|\psi\rangle$ is given by the following formula:

$$C(\psi) = |\lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2|. \tag{18}$$

Suppose now we choose $|\Phi\rangle$ to be one of $\{|\Phi_k\rangle : 1 \leq k \leq 4\}$, say $|\Phi_4\rangle$. Then any vector from $\{|\Phi\rangle\}^\perp$ should be a linear combination of $\{|\Phi_1\rangle, |\Phi_2\rangle, |\Phi_3\rangle\}$. As a direct consequence, we have the following interesting lemma which connects the concurrences of orthonormal bases of $\{|\Phi\rangle\}^\perp$ to 3×3 unitary matrices.

Lemma 6: Let $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ be an orthogonal basis for $\{|\Phi\rangle\}^\perp$, then there exists a 3×3 unitary matrices $U = [u_{kl}]_{3\times3}$ such that

$$C(\psi_1) = |u_{11}^2 + u_{12}^2 + u_{13}^2|, \tag{19}$$
$$C(\psi_2) = |u_{21}^2 + u_{22}^2 + u_{23}^2|, \tag{20}$$
$$C(\psi_3) = |u_{31}^2 + u_{32}^2 + u_{33}^2|. \tag{21}$$

Conversely, for any unitary matrix $U = [u_{kl}]_{3\times3}$, there exists an orthogonal basis for $\{|\Phi\rangle\}^\perp$, say $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ such that Eq. (19) holds.

Motivated by the above lemma, let $\mathcal{P}_1$ be the set of $x \in \mathcal{R}^3$ such that there exists a unitary matrix $U = [u_{kj}]_{3\times3}$ such that

$$x_1 = |u_{11}^2 + u_{12}^2 + u_{13}^2|, \tag{22}$$
$$x_2 = |u_{21}^2 + u_{22}^2 + u_{23}^2|, \tag{23}$$
$$x_3 = |u_{31}^2 + u_{32}^2 + u_{33}^2|. \tag{24}$$

Then it is clear that $\mathcal{P}_1$ is exactly the set of points corresponding to the concurrences of the orthogonal bases of $\{|\Phi\rangle\}^\perp$. Let $\mathcal{P}_2$ be the set of $x \in \mathcal{R}^3$ satisfying the following equations:

$$x_1 + x_2 + x_3 \geq 1, \tag{25}$$
$$x_1 + x_2 - x_3 \leq 1, \tag{26}$$
$$x_2 + x_3 - x_1 \leq 1, \tag{27}$$
$$x_3 + x_1 - x_2 \leq 1, \tag{28}$$
$$0 \leq x_1, x_2, x_3 \leq 1. \tag{29}$$

Obviously, $\mathcal{P}_2$ is just a unit regular tetrahedron. We shall show that $\mathcal{P}_2$ is contained by $\mathcal{P}_1$. That means any point of the regular tetrahedron corresponds to some orthonormal basis of $\{|\Phi\rangle\}^\perp$.

Theorem 8: $\mathcal{P}_2 \subseteq \mathcal{P}_1$.

Proof. For any point $x \in \mathcal{P}_2$, we shall construct a 3×3 unitary operation U such that Eq. (22) holds. Without loss of generality, we may assume $x_1 \geq x_2 \geq x_3 \geq 0$. So Eq. (25) is reduced to the following equations:

$$x_1 + x_2 + x_3 \geq 1, \tag{30}$$
$$x_1 + x_2 - x_3 \leq 1, \tag{31}$$
$$0 \leq x_3 \leq x_2 \leq x_1 \leq 1. \tag{32}$$

Construct a unitary matrix U as follows:

$$U = \begin{pmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{i\theta} & 0 \\ 0 & 0 & e^{i\theta} \end{pmatrix},$$

where $[u_{kl}]_{3\times3}$ is a real orthogonal matrix, and $0 \leq \theta \leq \pi$. By a simple calculation, we have

$$U = \begin{pmatrix} u_{11} & u_{12}e^{i\theta} & u_{13}e^{i\theta} \\ u_{21} & u_{22}e^{i\theta} & u_{23}e^{i\theta} \\ u_{31} & u_{32}e^{i\theta} & u_{33}e^{i\theta} \end{pmatrix}.$$

Our purpose is to choose suitable real numbers u_{11}, u_{21}, u_{31}, and θ such that

$$u_{11}^2 + (1 - u_{11}^2)e^{2i\theta} = x_1, \tag{33}$$
$$u_{21}^2 + (1 - u_{21}^2)e^{2i\theta} = x_2, \tag{34}$$
$$u_{31}^2 + (1 - u_{31}^2)e^{2i\theta} = x_3, \tag{35}$$
$$u_{11}^2 + u_{21}^2 + u_{13}^2 = 1. \tag{36}$$

From the first three equations, we have

$$u_{1k}^2 = \frac{\sin\theta \pm \sqrt{x_k^2 - \cos^2\theta}}{2\sin\theta}, \ k = 1, 2, 3. \tag{37}$$

We shall choose a suitable θ such that the last normalized relation holds. That is, choose θ such that

$$\sin\theta \pm \sqrt{x_1^2 - \cos^2\theta} \pm \sqrt{x_2^2 - \cos^2\theta} \pm \sqrt{x_3^2 - \cos^2\theta} = 0,$$

where $\cos^{-1}(x_3) \leq \theta \leq \pi/2$. The difficulty here is how to choose suitable signs for u_{1k}. Let

$$f(\theta) = \sin\theta - \sqrt{x_1^2 - \cos^2\theta} - \sqrt{x_2^2 - \cos^2\theta} - \sqrt{x_3^2 - \cos^2\theta},$$
$$g(\theta) = \sin\theta - \sqrt{x_1^2 - \cos^2\theta} - \sqrt{x_2^2 - \cos^2\theta} + \sqrt{x_3^2 - \cos^2\theta}.$$

It is clear that

$$f(\frac{\pi}{2}) = 1 - x_1 - x_2 - x_3 \leq 0, \quad (38)$$

$$g(\frac{\pi}{2}) = 1 + x_3 - x_1 - x_2 \geq 0, \quad (39)$$

$$f(\cos^{-1}(x_3)) = g(\cos^{-1}(x_3)) \in \mathcal{R}, \quad (40)$$

from which we have

$$f(\frac{\pi}{2}).g(\frac{\pi}{2}) \leq 0 \text{ and } f(\cos^{-1}(x_3)).g(\cos^{-1}(x_3)) \geq 0. \quad (41)$$

Noticing that $f(\theta)g(\theta)$ is a real-valued function of θ, we conclude by the intermediate value theorem that there exists $\cos^{-1}(x_3) \leq \theta_0 \leq \frac{\pi}{2}$ such that $f(\theta_0)g(\theta_0) = 0$. So $f(\theta_0) = 0$ or $g(\theta_0) = 0$. Without loss of generality, assume $g(\theta_0) = 0$, then we can choose u_{11}, u_{21}, u_{31} as follows:

$$u_{11} = \sqrt{\frac{\sin\theta_0 - \sqrt{x_1^2 - \cos^2\theta_0}}{2\sin\theta_0}}, \quad (42)$$

$$u_{21} = \sqrt{\frac{\sin\theta_0 - \sqrt{x_2^2 - \cos^2\theta_0}}{2\sin\theta_0}}, \quad (43)$$

$$u_{31} = \sqrt{\frac{\sin\theta_0 + \sqrt{x_2^2 - \cos^2\theta_0}}{2\sin\theta_0}}. \quad (44)$$

By extending (u_{11}, u_{21}, u_{31}) into an real orthogonal matrix we obtain other entries u_{kl}. With that we complete the proof of $\mathcal{P}_2 \subseteq \mathcal{P}_1$. ■

We strongly believe that it also holds $\mathcal{P}_1 \subseteq \mathcal{P}_2$, thus $\mathcal{P}_1 = \mathcal{P}_2$. However, we don't know how to give a rigorous proof for this up to now.

ACKNOWLEDGEMENT

We thank Z.-F. Ji, G.-M. Wang, J.-X. Chen, Z.-H. Wei, and C. Zhang for helpful conversations. R. Duan acknowledges J. Walgate for interesting discussions at QIP 2007.

REFERENCES

[1] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, "Quantum nonlocality without entanglement," *Phys. Rev. A*, vol. 59, no. 2, pp. 1070–1091, 1999.

[2] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B.M. Terhal, "Unextendible product bases and bound entanglement," *Phys. Rev. Lett.*, vol. 82, no. 26, pp. 5385–5388, 1999.

[3] D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B.M. Terhal, "Unextendible product bases, uncompletable product bases and bound entanglement," *Comm. Math. Phys.*, vol. 238, pp. 379–410, 2003.

[4] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, "Local Distinguishability of multipartite orthogonal quantum states," *Phys. Rev. Lett.*, vol. 85, no. 23, pp. 4972–4975, 2000.

[5] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham, "Optimal local discrimination of two multipartite pure states," *Phys. Lett. A*, vol. 288, no. 2, pp. 62–68, 2001.

[6] Y.-X. Chen and D. Yang, "Optimally conclusive discrimination of nonorthogonal entangled states by local operations and classical communications," *Phys. Rev. A*, vol. 65, no. 2, 022320, 2002.

[7] M. Hillery and J. Mimih, "Distinguishing two-qubit states using local measurements and restricted classical communication," *Phys. Rev. A*, vol. 67, no. 4, 042304, 2003.

[8] Z. Ji, H. Cao, and M. Ying, "Optimal conclusive discrimination of two states can be achieved locally," *Phys. Rev. A*, vol. 71, no. 3, 032323, 2005.

[9] A. Acín, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz-Tapia, "Multiple-copy two-state discrimination with individual measurements," *Phys. Rev. A*, vol. 71, no. 3, 032338, 2005.

[10] Y. Ogata, "Local distinguishability of quantum states in infinite-dimensional systems," *J. Phys. A: Math. Gen.*, vol. 39, no. 12, pp. 3059-3069, 2006.

[11] J. Walgate and L. Hardy, "Nonlocality, asymmetry, and distinguishing bipartite states," *Phys. Rev. Lett.*, vol. 89, no. 14, 147901, 2002.

[12] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, "Hiding bits in Bell states," *Phys. Rev. Lett.*, vol. 86, pp. 5807–5810, 2001.

[13] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, "Quantum data hiding," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 580–598, 2002.

[14] T. Eggeling and R. F. Werner, "Hiding Classical Data in Multipartite Quantum States," *Phys. Rev. Lett.*, vol. 89, no. 9, 097905, 2002.

[15] A. Chefles, "Condition for unambiguous state discrimination using local operations and classical communication," *Phys. Rev. A*, vol. 69, no. 5, 050307(Rapid communications), 2004.

[16] S. Bandyopadhyay and J. Walgate, "Local distinguishability of any three quantum states," quant-ph/0612013, 2006.

[17] M. Nathanson, "Distinguishing bipartitite orthogonal states using LOCC: best and worst cases," *J. Math. Phys.*, vol. 46, no. 6, 062103, 2005.

[18] M. Owari and M. Hayashi, "Local copying and local discrimination as a study for non-locality of a set," *Phys. Rev. A*, vol. 74, no. 3, 032108, 2006. See also quant-ph/0411143 for a preliminary version.

[19] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, "Distinguishability of Bell states," *Phys. Rev. Lett.*, vol. 87, no. 27, 277902, 2001.

[20] H. Fan, "Distinguishability and indistinguishability by local operations and classical communication," *Phys. Rev. Lett.*, vol. 92, no. 17, 177905, 2004.

[21] J. Watrous, "Bipartite subspaces having no bases distinguishable by local operations and classical communication," *Phys. Rev. Lett.*, vol. 95, no. 8, 080505, 2005.

[22] P. Hayden and C. King, "Correcting quantum channels by measuring the environment," *Quantum Inf. Comput.*, vol. 5, no. 2, 156–160, 2005.

[23] M. Hayashi, D. Markham, M. Murao, M. Owari, and S. Virmani, "Bounds on multipartite entangled orthogonal state discrimination using local operations and classical communication," *Phys. Rev. Lett.*, vol. 96, no. 4, 040501, 2006.

[24] R. Y. Duan, Y. Feng, Z. F. Ji, and M. S. Ying, "Distinguishing arbitrary multipartite basis unambiguously using local operations and classical communication," *Phys. Rev. Lett.*, vol. 98, no. 23, 230502, 2007.

[25] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, "Local indistinguishability: More nonlocality with less entanglement," *Phys. Rev. Lett.*, vol. 90, no. 4, 047902, 2003.

[26] P.-X. Chen and C.-Z. Li, "Orthogonality and distinguishability: Criterion for local distinguishability of arbitrary orthogonal states," *Phys. Rev. A*, vol. 68, no. 6, 062107, 2003.

[27] S. M. Cohen, "Local distinguishability with preservation of entanglement," *Phys. Rev. A*, vol. 75, no. 5, 052313, 2007.

[28] Y. Feng and Y. Shi, "Characterizing locally distinguishable orthogonal product states," arXiv:0707.3581[quant-ph], 2007.

[29] V. Gheorghiu and R. B. Griffiths, "Entanglement transformations using separable operations," *Phys. Rev. A*, vol. 76, no. 3, 032310, 2007, a preliminary version is available at arXiv: 0705.0369v1[quant-ph].

[30] J. Eisert and H. J. Briegel, "Schmidt measure as a tool for quantifying multiparticle entanglement," *Phys. Rev. A*, vol. 64, no. 2, 022306, 2001.

[31] A. Acin, A. Andrianov, L. Costa, E. Jane, J.I. Latorre, R. Tarrach, "Generalized Schmidt Decomposition and Classification of Three-Quantum-Bit States," *Phys. Rev. Lett.*, vol. 85, no. 7, 85, pp. 1560 - 1563, 2000.

[32] B. M. Terhal and P. Horodecki, "Schmidt number for density matrices," *Phys. Rev. A*, vol. 61, no. 4, 040301(Rapid communications), 2000.

[33] It was intrdouced in Ref. [2] that a set of orthogonal product states $\mathcal{S}$ is completable if it can be extended into an orthogonal product basis of $\mathcal{H}$ (or local extension $\mathcal{H}_{ext} = \otimes_{k=1}^{K}(\mathcal{H}_k \oplus \mathcal{H}'_k)$ of $\mathcal{H}$). Here we generalize this notion by allowing $\mathcal{S}$ is an arbitary set of orthogonal separable projecors such that the projector on the orthogonal complement of $\mathcal{S}$ is again separable.

[34] P. Horodecki, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, "Rank two bipartite. bound entangled states do not exist," *Theor. Comput. Sci.*, vol. 292, no. 3, pp. 589–596, 2003.

[35] W. K. Wootters, "Entanglement of formation of an arbitrary state of two qubits," *Phys. Rev. Lett.*, vol. 80, no. 10, pp. 2245–2248, 1998.

[36] A. Winter, "On environment-assisted capacities of quantum channels," arXiv:quant-ph/0507045v1, 2005.